FOCUS ONTARIO

A YEAR OF OUTREACH, ENGAGEMENT AND COLLABORATION

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

2015 ANNUAL REPORT

June 27, 2016

The Honourable Dave Levac
Speaker of the Legislative Assembly of Ontario

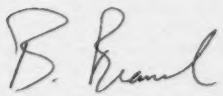
Dear Speaker,

I have the honour to present the 2015 Annual Report of the Information and Privacy Commissioner of Ontario to the Legislative Assembly.

This report covers the period from January 1 to December 31, 2015.

Please note that additional reporting from 2015, including the full array of statistics, analysis and supporting documents, may be found within our online Annual Report section at www.ipc.on.ca.

Sincerely yours,



Brian Beamish
Commissioner

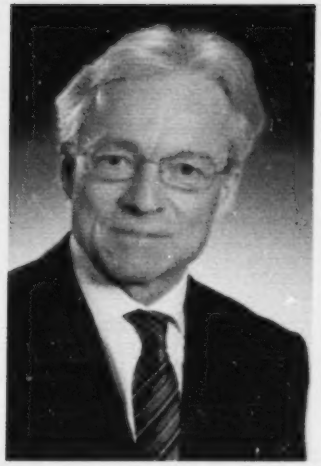
TABLE OF CONTENTS

COMMISSIONER'S MESSAGE 1
ABOUT US 5
OUR WORK 6
ACCESS 8
- POSITIVE STEPS FORWARD 8
- OPEN CONTRACTING 8
- SUPPORT FOR INSTITUTIONS 9
- CHANGES TO RECORD KEEPING LAWS 9
- ACCESS INVESTIGATION PROVIDES GUIDANCE FOR INSTITUTIONS 10
- SIGNIFICANT ACCESS DECISIONS 10
- JUDICIAL REVIEWS 14

PRIVACY 16
- POLICE RECORD CHECKS 16
- STREET CHECKS 17
- BODY-WORN CAMERAS 17
- "YES, YOU CAN" 18
- SITUATION TABLES 18
- SIGNIFICANT PRIVACY COMPLAINTS 19
- KEY PRIVACY PUBLICATIONS 20

HEALTH PRIVACY 22
- *PHIPA*–A PRESCRIPTION FOR PRIVACY 22
- PROTECTING PATIENT PRIVACY 23
- E-PHIPA (BILL 119) 23
- SIMPLIFIED *PHIPA* PROCESSES 24
- SIGNIFICANT *PHIPA* DECISIONS 24
- HEALTH PRIVACY PUBLICATIONS 25

MEDIATION 27
CONSULTATIONS 29
COMMISSIONER'S RECOMMENDATION 30
STATISTICS 33
FINANCIAL SUMMARY 39



A Year of Outreach, Engagement and Collaboration

When I began my term as Information and Privacy Commissioner, I committed to increased engagement with institutions and individuals from every corner of Ontario, and to making significant efforts to strengthen existing relationships while forging new ones. I am happy to report that 2015 was a tremendously successful year as my office continued to build connections across the province in the spirit of proactive engagement and collaboration.

In 2015, we revived our Reaching Out to Ontario program with the goal of meeting face-to-face with institutions and public servants across Ontario. I had the opportunity, along with my staff, to visit St. Catharines, Ottawa and Sault Ste. Marie, where we hosted events to discuss current and emerging access to information and privacy issues. Hundreds of people attended these events and we received very positive feedback, not only for our informative sessions, but also for our efforts in actively reaching out to these communities. This year, we also accepted invitations to participate in over 60 conferences and presentations. While we are unable to accept every request, we make a sincere effort to appear at as many events as possible to discuss the wide and complex range of issues that affect access to information and privacy. Some of the organizations we visited over the past year include the Ontario Hospital Association, Trillium Health Partners, the

Hundreds of people attended these events and we received very positive feedback, not only for our informative sessions, but also for our efforts in actively reaching out to these communities.

Ontario Bar Association, the Association of Municipal Managers, Clerks and Treasurers of Ontario and the Ontario Association of Chiefs of Police.

This year we referred more cases than ever to the Attorney General for prosecution under the *Personal Health Information Protection Act* and continued our work with the Ministry of Health and Long-Term Care on updating and strengthening Ontario's health privacy laws. Additionally, we provided advice and commentary to many police services, the Ministry of Community Safety and Correctional Services, and a number of community groups, on the access and privacy implications of police record checks and street checks.

Requests for our participation in consultations and working groups continued to increase, with our office receiving a record number in 2015. In responding to these requests for advice and comment, we take a collaborative approach that balances the business needs of institutions with the public's access and privacy rights. We focus on providing useful guidance to help institutions understand their legislative obligations and how to appropriately address access and privacy issues. Further, we frequently share the lessons of our decisions and collaborative work by turning them into practical guidance materials. In 2015, we published a number of papers, including: *Transparency, Privacy and the Internet – Municipal Balancing Acts*; *Open Contracting – Proactive Disclosure of Procurement Records*; and *Detecting and Deterring Unauthorized Access to Personal Health Information*.

This year we also extended our public outreach through a joint effort with the Office of the Provincial Advocate for Children and Youth. *Yes, You Can – Dispelling the Myths About Sharing Information with Children's Aid Societies* is a guide to help professionals understand that their ability to share information with a children's aid society when they suspect a child may be at risk of harm is not restricted by privacy legislation. To my knowledge, this was the first time that two independent officers of the Ontario Legislature have worked together on an issue of great public interest. I look forward to using this model for future public awareness campaigns.

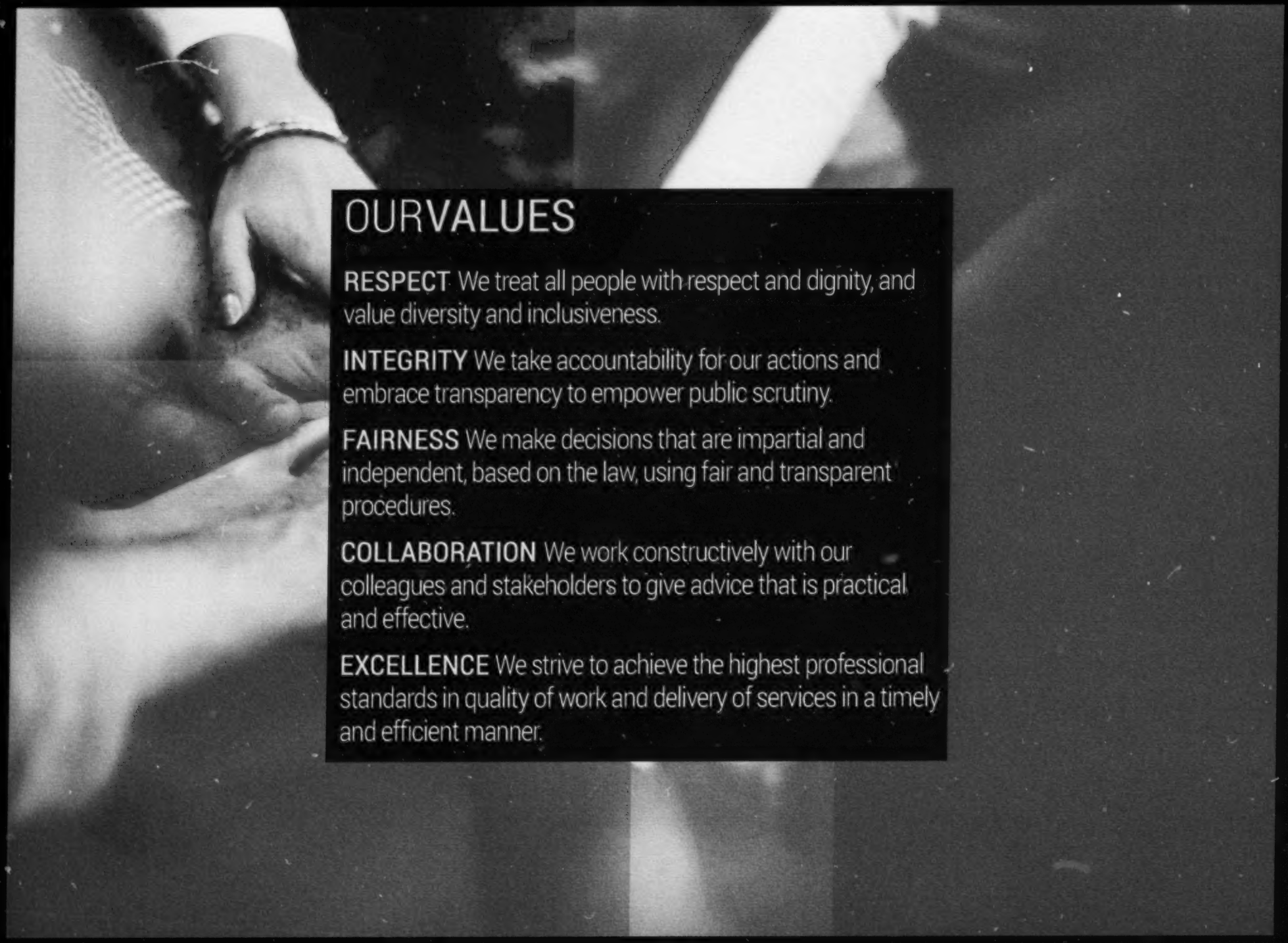
The IPC commitment to collaboration and cooperation also extended to our work in resolving and deciding access to information appeals and privacy complaints. Our office was particularly successful this year in resolving a significant number of appeals and complaints through mediation, without the need for an adjudicated decision. Not only does this approach benefit the parties, but it also allows my office to process an increasing number of appeals and complaints using existing resources.

The IPC remains committed to the cause of Open Government in Ontario. Open Data and Open Information policies hold the promise of creating a more open and accountable government, as well as fueling the information economy by providing start-up companies and entrepreneurs with ready access to public data. These policies also offer increased efficiency by reducing the need for institutions to reactively respond to requests for information.

The IPC will continue to work with these institutions to help them meet their goals in compliance with access and privacy laws. Ultimately, collaboration and cooperation allows us to achieve our goal of furthering the public interest.

The IPC will soon begin its fourth decade of service to the people of Ontario. We remain committed to building on the lessons of the past so that we can safeguard the future of access and privacy rights in Ontario.

Brian Beamish
Commissioner



OUR**VALUES**

RESPECT We treat all people with respect and dignity, and value diversity and inclusiveness.

INTEGRITY We take accountability for our actions and embrace transparency to empower public scrutiny.

FAIRNESS We make decisions that are impartial and independent, based on the law, using fair and transparent procedures.

COLLABORATION We work constructively with our colleagues and stakeholders to give advice that is practical and effective.

EXCELLENCE We strive to achieve the highest professional standards in quality of work and delivery of services in a timely and efficient manner.

Our Strategic Goals

Uphold the public's right to know and right to privacy.

Encourage open, accountable and transparent public institutions.

Promote privacy protective programs and practices.

Ensure an efficient and effective organization with engaged and knowledgeable staff.

Empower the public to exercise its access and privacy rights.

Our Office

Established in 1987, the Office of the Information and Privacy Commissioner of Ontario (IPC) provides independent oversight of the province's access and privacy laws.

THE *FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT*

The *Freedom of Information and Protection of Privacy Act* (*FIPPA*) applies to over 300 provincial institutions such as ministries, provincial agencies, boards and commissions, as well as community colleges, universities, local health integration networks and hospitals.

THE *MUNICIPAL FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT*

The *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) applies to over 1,200 municipal institutions such as municipalities, police services boards, school boards, conservation authorities, boards of health and transit commissions.

THE *PERSONAL HEALTH INFORMATION PROTECTION ACT*

The *Personal Health Information Protection Act* (*PHIPA*) covers individuals and organizations in Ontario that are involved in the delivery of health care services, including hospitals, pharmacies, laboratories, and Ontario's Ministry of Health and Long-Term Care, as well as health care providers such as doctors, dentists and nurses.

Commissioner

The Commissioner is appointed by the Legislative Assembly of Ontario and is independent of the government of the day. His mandate includes resolving access to information appeals and privacy complaints, educating the public about access and privacy issues, reviewing information practices and commenting on proposed legislation, programs and practices.

Tribunal

INTAKE

The Registrar receives all access appeals and privacy complaints, including health privacy complaints, and directs them to the appropriate department. Intake often screens out or resolves appeals or complaints at an early stage. Our intake analysts also serve as our front line response to privacy breaches.

INVESTIGATION AND MEDIATION

Our team of investigators gather information and resolve privacy complaints, including health privacy complaints. Our team of *FIPPA* and *MFIPPA* mediators work to resolve or narrow the issues in access appeals. While our decisions attract the most attention, the majority of access appeals and privacy complaints are resolved through mediation.

ADJUDICATION

When a resolution cannot be found through mediation, access appeals and health complaints are forwarded to an adjudicator who will decide whether or not to conduct a formal inquiry. The adjudicator collects and reviews evidence and arguments and issues a final and binding decision. A court review of IPC decisions is available in some limited circumstances.

Legal

Our legal department works in close collaboration with and provides legal advice and support to the Commissioner and other departments. Our lawyers frequently provide advice and comments with respect to proposed legislation, programs and technologies in the government and health sectors. They also represent the Commissioner in judicial reviews and appeals of the IPC's decisions and in other court cases regarding access to information and privacy issues.

Policy

Our policy analysts research, analyze and provide advice on current, evolving and emerging access and privacy issues. They are routinely asked to examine and review the access and privacy practices of public organizations. They also examine and provide comments on any proposed legislation that may impact the rights of Ontarians.

Health Policy

Our health policy team researches privacy issues relating to personal health information and provides guidance through education, consultation, and comment on health policy and legislation. They also conduct reviews of the information

practices of prescribed entities and persons on a tri-annual basis.

Communications

Communications promotes the work of the IPC by engaging in public information campaigns and outreach initiatives to both the public and public servants. Our website, social media, media relations, and public events are managed by the communications team.

Corporate Services and Technology

From overseeing organizational operations such as human resources and monitoring expenditures to providing technical support, our Corporate Services and Technology department provides the day-to-day operational support and infrastructure needed for the Commissioner and IPC staff to do their jobs effectively and efficiently.

OUR WORK IN 2015

COMMISSIONER
In 2015, the IPC was mentioned more than 400 times in the media and the Commissioner made over 25 appearances and presentations.
LEGAL SERVICES
Made more than 30 presentations
Represented the Commissioner in four judicial review hearings.
POLICY
Released 7 guidance documents
Provided advice to a variety of public sector organizations. Participated in a number of public events where they provided information and insight on privacy and access issues.
HEALTH POLICY
Issued 4 publications
Helped develop amendments to health privacy legislation. Consulted with and presented to numerous organizations.
COMMUNICATIONS
Fielded 140 media calls
Oversaw four major events that attracted over 500 people. Responds to thousands of calls and emails from the public through our public enquiry lines each year.
TRIBUNAL SERVICES
INTAKE
OUR REGISTRAR RECEIVED
6%
5%
1,403 ACCESS APPEALS, AN INCREASE OVER 2014
460 HEALTH COMPLAINTS, AN INCREASE OVER 2014
276 PRIVACY COMPLAINTS, SLIGHTLY LESS THAN 280 RECEIVED IN 2014
262 PRIVACY
399 HEALTH PRIVACY
COMPLAINTS
CLOSED AT INTAKE
INVESTIGATION & MEDICATION
ACCESS APPEALS
69%
83%
*PRIVACY COMPLAINTS
69% OF ACCESS APPEALS AND 83% OF *PRIVACY COMPLAINTS THAT WERE REFERRED TO MEDIATION WERE SETTLED.
*including health privacy complaints
ADJUDICATION
121 PROVINCIAL ORDERS
127 MUNICIPAL ORDERS
5 PHIPA DECISIONS
ISSUED BY OUR OFFICE

Access to Information

Central to the concept of Open Government is Open by Default—the idea that government-held information is open to public scrutiny unless there is a compelling reason for it to remain unpublished. This means making as much information as possible available to the public through proactive disclosure—and not waiting to be asked. Open Government complements our access to information legislation by promoting the release of information, in a manner that is easily accessible to the public, while reserving the formal access to information process for cases that may involve personal or other confidential information.

One of the key purposes of the Freedom of Information and Protection of Privacy Act *(FIPPA) and its municipal counterpart (MFIPPA) is to provide the public with a right of access to government information, with very few exceptions. Our office strongly supports* **Open Government** *policies and believes government institutions must be as transparent and accountable as possible.*

Positive Steps Forward

In our 2014 annual report, we commended the Open Government Engagement Team for its Open by Default report and encouraged the province to move forward with its recommendations. Ontario's Treasury Board Secretariat made great strides by engaging with the public on a draft Open Data Directive in November. While commending the province for its work on the directive, released in April 2016, we offered a number of recommendations for amendments to ensure that the government's approach to Open Data respects the privacy rights of individuals. We recommended that the directive:

- highlight the need to protect personal information before opening data
- require de-identified data sets to be periodically reviewed so that they cannot be used to re-identify individuals
- ensure that descriptions of data sets are accessible and understandable to the public
- include requirements to further open the province's procurement process

Open Contracting

We were pleased to see that the province accepted our recommendation to publish contract information as Open Data. Under the Open Data Directive, information such as the winning bid for every contract (for example, vendor name, financial payment information), will be included in Open Data and published in a timely manner, unless excluded. In new government contracts, vendors must agree that financial data of contracts are not considered commercially sensitive and may be released. To help implement this, we issued a guidance

document, *Open Contracting: Proactive Disclosure of Procurement Records*. It explains the benefits of proactive disclosure and offers tips on designing and implementing a transparent procurement process, while still protecting confidentiality where appropriate. The IPC is pleased to see these policies and practices implemented, since they strengthen transparency and accountability around government spending. This practice will also help reduce the number of procurement-related freedom of information requests and appeals, along with their associated costs.

RECOMMENDATION

Information about contracts awarded should be published in a timely manner.

Support for Institutions

Our work on Open Government, and open procurement in particular, has sparked a lively and constructive conversation with provincial and municipal government staff that we expect to continue in the coming years. We actively support openness initiatives in the province by providing advice and comment on consultation papers and by engaging with the professionals who are implementing open government in institutions. We look forward to learning more about their challenges and assisting them as they move toward greater accountability and transparency.

Changes to Recordkeeping Laws

Another important step towards a more open government was taken on January 1, 2016, when Bill 8, the *Public Sector and MPP Accountability and Transparency Act, 2014*, became law. Bill 8 amends *FIPPA* and *MFIPPA* to include requirements for institutions to ensure the preservation of records. As a result of the amendments, heads of institutions are now required to take "reasonable measures" to preserve records in their custody or control. The amendments apply to all stages of the information life cycle and make it an offence to alter, conceal or destroy a record with the intention of denying access. As the agency that oversees compliance with *FIPPA* and *MFIPPA*, the IPC strongly supports these amendments, knowing that the right of access depends on the appropriate management and preservation of records. These amendments reflected some of the recommendations from our 2013 special investigation report, *Deleting Accountability: Records Management Practices of Political Staff*. To help institutions understand their new responsibilities, and develop and implement plans to address these provisions, we released a paper, *Bill 8: The Recordkeeping Amendments*.

RECOMMENDATION

Every institution should have well-documented procedures in place for responding to requests for information and follow them every time. Training should be provided to all staff who respond to requests and those who are regularly involved in record searches.

Access Investigation Provides Guidance for Institutions

After reports in the media about the Toronto District School Board's access to information processes, the IPC started an investigation involving allegations of misconduct related to a request for trustee expense audit documents. In Order MO-3230, we found that a lack of clarity about the records requested and a failure, on the part of the board, to follow internal procedures led to challenges in responding to the request. This case should serve as a cautionary tale for all institutions in managing requests for access to records.

Ontario's provincial and municipal access laws place important responsibilities on freedom of information staff, who must ask for clarification when a request is unclear. Failure to take this important step can result in misunderstanding and delays.

Significant Access Decisions

Our office issued a number of decisions this year which gave direction on how *FIPPA* and *MFIPPA* should be applied. Some highlights include:

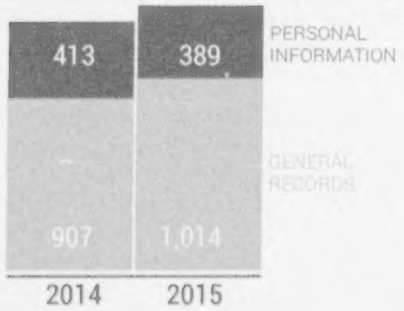
PO-3458

The Ontario Lottery and Gaming Corporation received a request from a business owner for information regarding allegations—about her and her business—made by her sister. The request was denied as personal information was included within the records. We determined that, even though the records contained personal information, the corporation should disclose the records because disclosure was not an unjustified invasion of privacy.

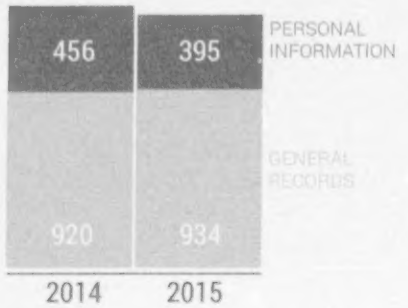
PO-3461

A reporter asked the Ministry of Community Safety and Correctional Services for records detailing when DNA samples were taken from victims and the addresses from where samples were taken, as part of a specific investigation. The reporter was initially denied access, but we determined that the information should be disclosed because a compelling public interest outweighed the privacy exemption.

APPEALS OPENED IN 2015



APPEALS CLOSED IN 2015



PO-3467

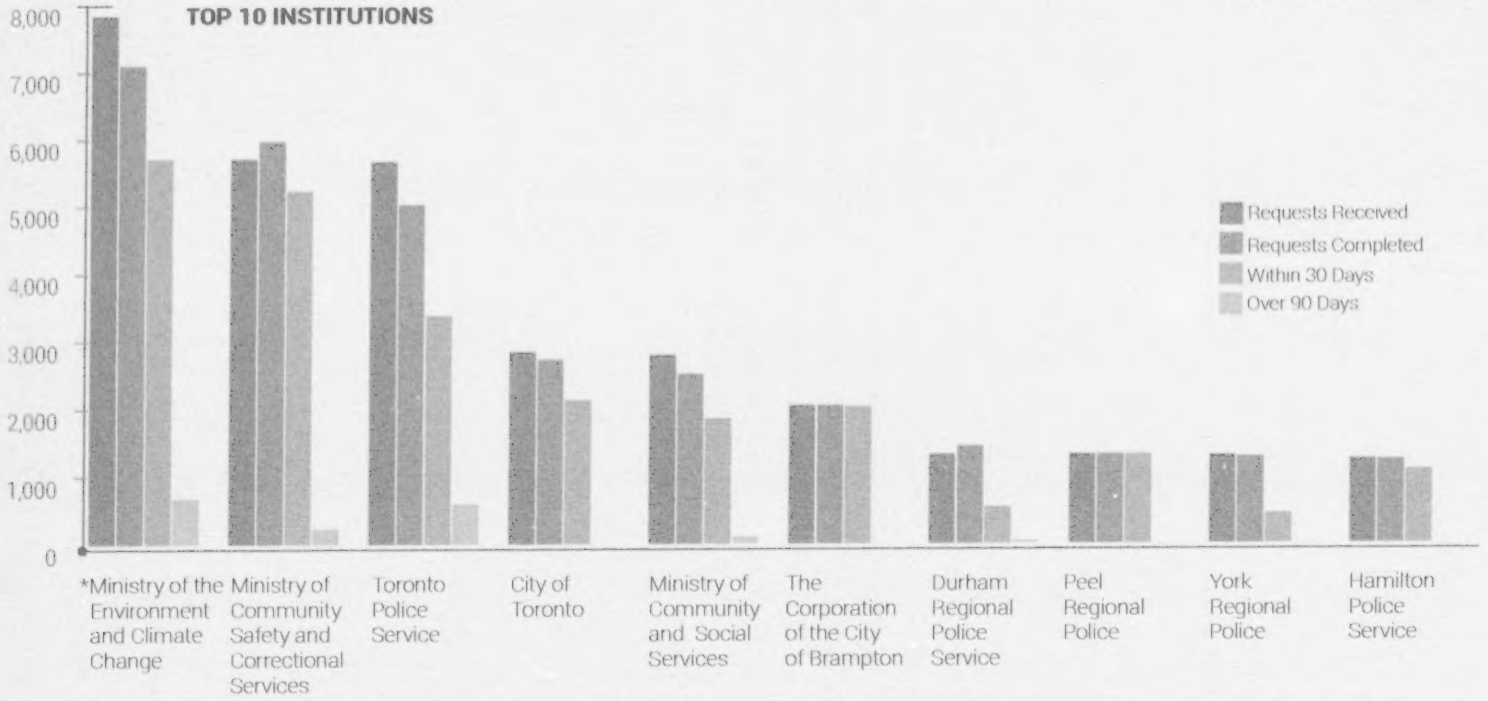
A requester asked the Ministry of Transportation for the names of driving instructors who have had their instructor licenses revoked, without the reasons for the revocation. We considered this information to be about the instructors in a business (rather than personal) capacity and ordered the ministry to disclose the names.

PO-3481

The Ministry of the Attorney General received a request about certain wrongfully convicted individuals and any applications for compensation made by those individuals. We upheld the ministry's decision to neither confirm nor deny the existence of records, since doing so would result in an unjustified invasion of personal privacy by, for example, potentially confirming that they did or did not apply for compensation.

PO-3487-I

Amnesty International made a multi-part request to the Ministry of Community Safety and Correctional Services for records relating to the Ontario Provincial Police's response to the Mohawk protest and occupation activities in 2007 and 2008. We determined that the ministry's search for two audio/video recordings of an identified individual's holding cell was not reasonable and ordered additional searches.



* Update July 18, 2016 : The Ministry of the Environment and Climate Change is currently reviewing its freedom of information request compliance rates as reported to the IPC.

MO-3178

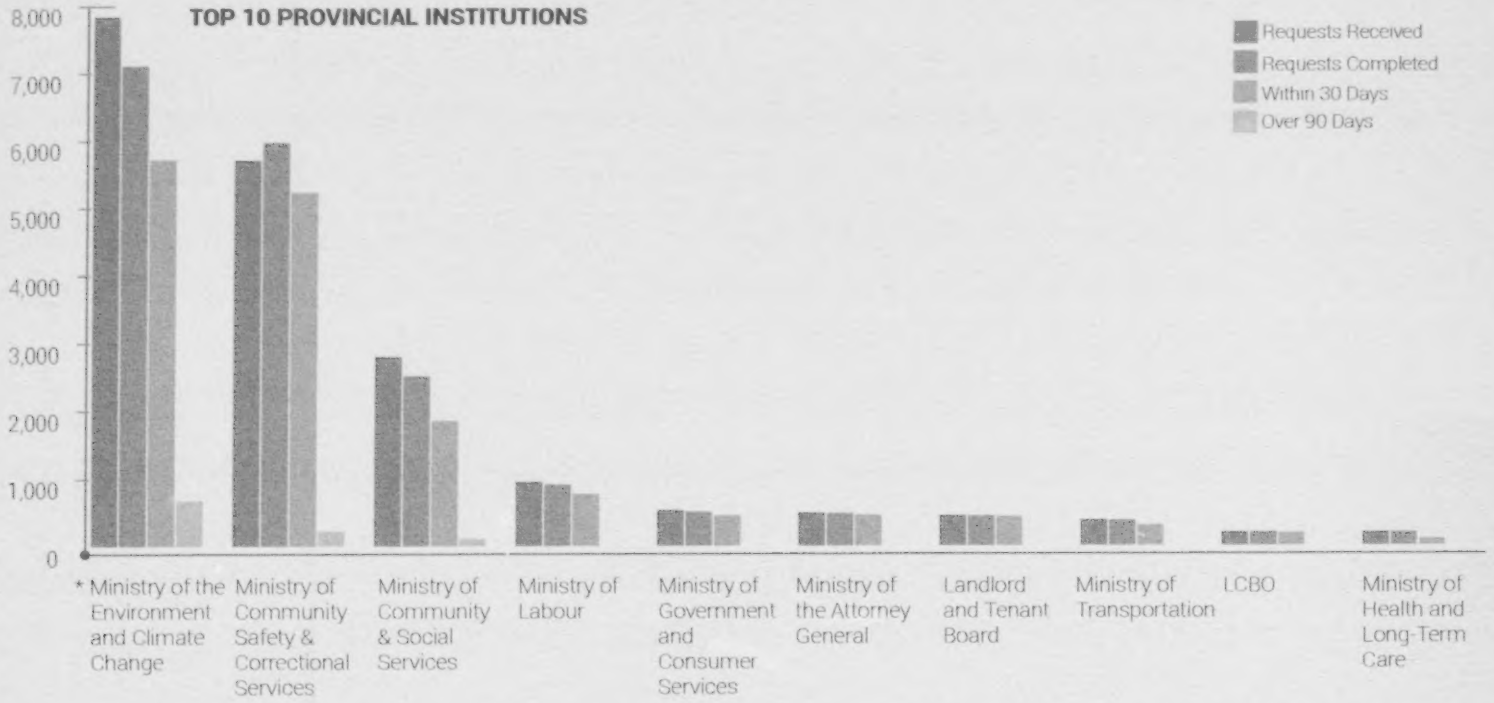
The York Catholic District School Board was asked for all negotiated leases relating to land that it leased to a third party, but it denied access. We decided no exemptions applied and ordered the leases disclosed.

MO-3181

A request was made for the employment contracts of two Deep River Police Services Board employees and the legal fees incurred when drafting the agreements. Though a number of exemptions were claimed, we found that the contents of these contracts should be disclosed.

MO-3228

The Toronto District School Board denied access to an audit report on the basis that disclosure would reveal the substance of deliberations of a closed meeting. We ordered the report to be released as we determined that the financial matters discussed did not qualify for the exemption.



* Update July 18, 2016: The Ministry of the Environment and Climate Change is currently reviewing its freedom of information request compliance rates as reported to the IPC.

MO-3238

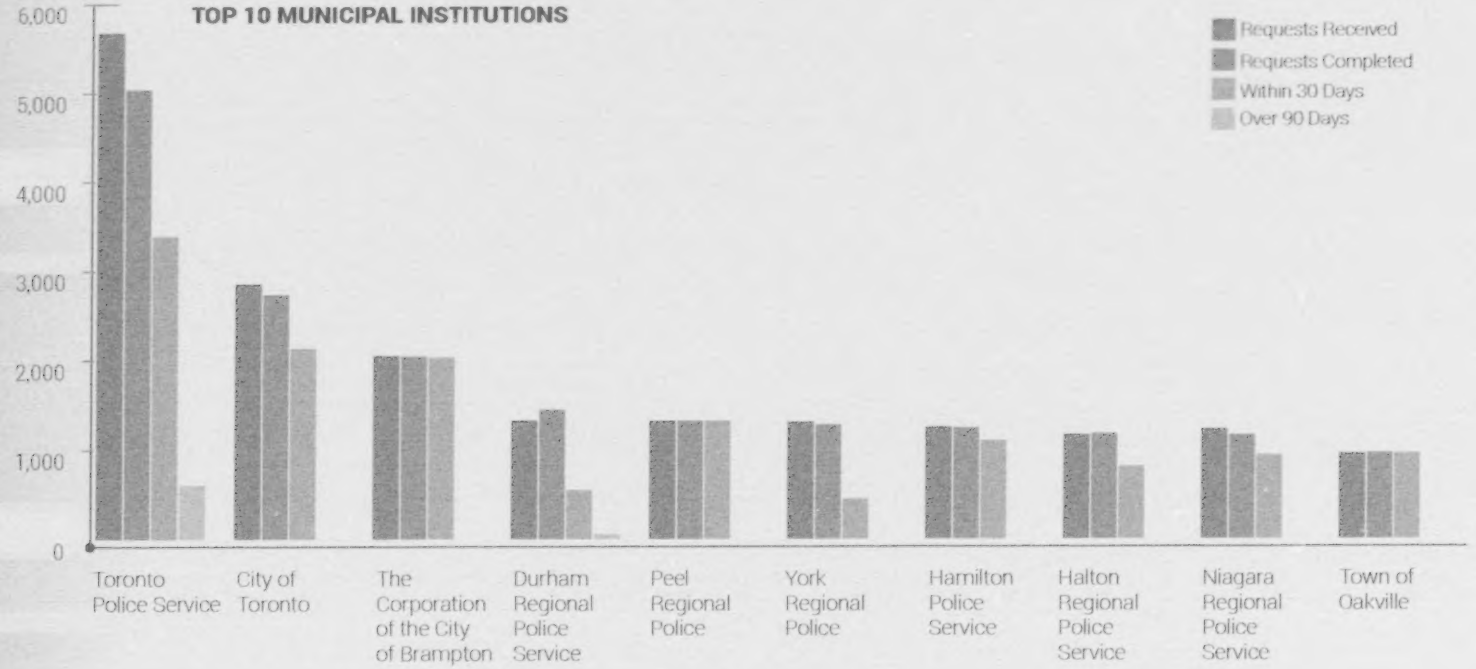
We decided that a Toronto Transit Commission surveillance tape of an alleged assault by a bus driver was covered by *MFIPPA*. We ordered disclosure of a severed copy of the tape, with the personal information of other identifiable individuals withheld.

MO-3239

The Kingston Police Services Board denied access to record check information, relying on the employment information exclusion. We decided that the exclusion did not apply and ordered the board to issue a revised access decision.

PO-3539

We upheld the decision of the Ministry of Children and Youth Services that multiple requests were frivolous and vexatious, since the actions of the requester established an abusive pattern of conduct. We limited the requester's right of access to one active appeal or request at a time.



Disclosure to the Children's Aid Society

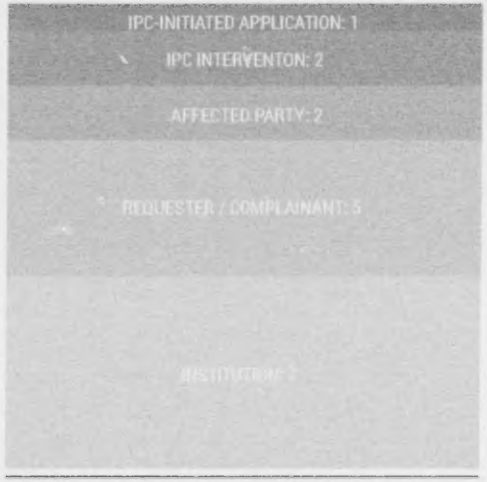
A children's aid society advised a police service of the presence of a potential caregiver in a home where the society had placed a vulnerable foster child, for the purpose of ensuring there were no safety concerns arising from that situation. The police then revealed to the society the existence of pending criminal charges against the potential caregiver for firearm and drug offences. The Commissioner concluded that the police properly disclosed this information to the society under *MFIPPA*, since the disclosure was made for the purpose of complying with the duty to report a child in need of protection under the *Child and Family Services Act*. On judicial review, the Divisional Court ruled that the Commissioner's decision was reasonable.

To promote awareness of the importance of sharing information with a children's aid society when there are reasons to believe a child may be at risk, the IPC published the guide, *Yes, You Can*, together with the Office of the Provincial Advocate for Children and Youth.

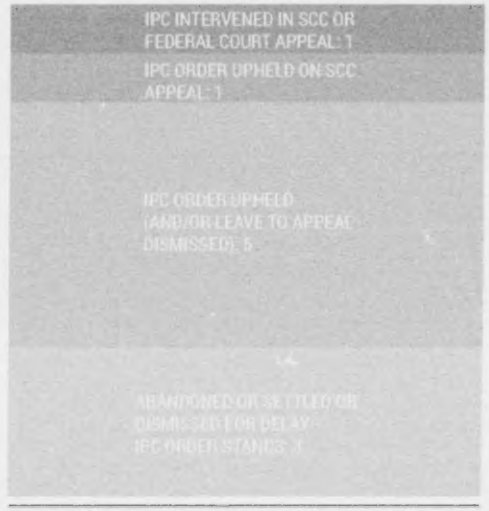
LCBO Wine Club Personal Information Collection

Order PO-3356-R directed the Liquor Control Board of Ontario (LCBO) to stop collecting the personal information of wine club members when a club submits orders for wine to the LCBO on the members' behalf. The LCBO claimed that it required this information to prevent fraud and to

New Judicial Review applications in 2015: 8



Outstanding Judicial Reviews as of December 31, 2015: 17


IPC INTERVENED IN SCC OR FEDERAL COURT APPEAL: 1
IPC ORDER UPHELD ON SCC APPEAL: 1
IPC ORDER UPHELD (AND/OR LEAVE TO APPEAL DISMISSED): 5

Judicial Reviews Closed and/or Heard in 2015: 10

comply with provincial liquor legislation and therefore, such collection was necessary to the proper administration of the LCBO's wine club program. The IPC found that, contrary to the LCBO's claims, the collection of personal information was not necessary for the proper administration of the program. On judicial review, the Divisional Court found the IPC's order to be reasonable.

Ontario Power Generation Contract Disclosures

Ontario Power Generation (OPG) denied a request for records related to engineering, procurement and construction agreements with two companies for the refurbishment of nuclear reactors. Order PO-3311 partially upheld OPG's decision, but ordered large portions of the contracts to be disclosed. The companies sought a judicial review, claiming that the contractual terms were confidential business information that they supplied to OPG. The Divisional Court dismissed the application, ruling that the IPC's interpretation and application of the third-party information exemption was "well articulated, justifiable, intelligent and transparent." The IPC has since published a guidance paper, *Open Contracting: Proactive Disclosure of Procurement Records*, which explains how the third-party information exemption has been applied to contractual agreements.

Employee Names in Family Responsibility Office Files

An individual asked for records contained in his Family Responsibility Office (FRO) case file. The Ministry of Community and Social Services agreed to disclose some records, but refused to disclose the full names of its employees and redacted those names where they appeared in the records.

In Order PO-2917, the IPC rejected the argument of the ministry and the Ontario Public Service Employees Union that employee names could be withheld based on the health and safety exemptions in *FIPPA*. Evidence was provided of general threats against FRO employees in other cases but there was no evidence suggesting that the requester was a threat to anyone. The IPC found that disclosure of this information could not reasonably be expected to threaten the safety or health of the employees and, therefore, the names should be disclosed.

The ministry sought judicial review of that decision, which was dismissed by the Divisional Court in February 2014. The matter was appealed to the Ontario Court of Appeal. Before that court, it was argued that the requester should not be allowed to know the names because he could post them on the internet and another person, after learning of the employee names, could then endanger them. In dismissing the appeal, the court reasoned that the risk that a requester will share information provided to him/her is *one* relevant factor in determining whether the evidentiary threshold for potential harm has been met in a given case. But in this case, the Court of Appeal upheld the IPC's finding that the employees were not entitled to remain anonymous because there was an insufficient basis to find that disclosure of this information could reasonably be expected to threaten the safety or health of these individuals.

Protection of Privacy

In the spirit of our ongoing commitment to collaboration, in 2015 the IPC consulted and provided advice on a number of privacy issues, including police record checks, street checks, body-worn cameras, situation tables and the sharing of information with children's aid societies. These important issues are described below.

Police Record Checks

Employers and other organizations often require job applicants and volunteers to consent to police record checks (PRCs). In late 2014, after a decade of hearing the IPC and others raise concerns about inconsistent, invasive and unfair PRC practices, the government signaled that it would introduce legislation to regulate their use.

In 2015, we worked closely with the province on the development of the proposed legislation. This legislation was based on an Ontario Association of Chiefs of Police PRC guideline that the IPC was also involved in creating.

In June 2015, the *Police Record Checks Reform Act*, or Bill 113, was introduced in the Legislature by Ontario's Minister of Community Safety and Correctional Services (MCSCS). The legislation establishes a new provincial standard that clarifies, limits and controls the scope of police record check disclosures to employers, volunteer agencies, and other third parties.

After second reading of Bill 113, the IPC presented a *Submission to the Standing Committee on Justice Policy*. We were generally very supportive of Bill 113, but we provided a number of recommendations on ways to better support privacy and enhance public confidence and transparency in the PRC process. We also committed to working with MCSCS on the development of regulations and guidance materials.

This legislation is the direct result and a great example of a collaborative approach to addressing significant public safety issues that raise privacy concerns. The new law reflects a balance between privacy and human rights and the needs of law enforcement that would not have been possible without the active involvement of many stakeholders.

Championing effective collaboration for greater public good was one of the key themes of our 2016 Privacy Day event. Our January symposium brought together members of the policing, privacy and human rights communities to talk about the importance of working together to find the balance between privacy and public safety.

FIPPA *and* MFIPPA *set the rules for how and when government organizations may collect, use, and disclose personal information. Our office has the authority to comment on proposed legislation and government programs to ensure they are designed in a way that protects privacy. These laws also allow us to investigate privacy complaints related to personal information held by government.*

We look forward to continuing this model of collaboration over the next year.

Street Checks

While street checks may sometimes be a necessary policing activity, they can also invade personal privacy and may result in discrimination and stigmatization. Without appropriate restrictions on street checks, sensitive personal information may be collected, used, and disclosed by the police, in violation of an individual's privacy and other rights.

A street check involves a police officer approaching an individual in a public space to ask for information such as their name, where they are going and what they are doing, in circumstances where they are not required to provide these details.

Since 2014, the IPC has been actively working with the Toronto Police Service (TPS) and its Police and Community Engagement Review (PACER) Committee to help them improve the TPS's street check practices.

In 2015, our office also participated in MCSCS's public consultations on the development of a draft regulation governing street check practices in Ontario.

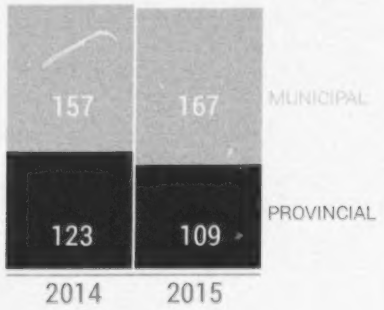
In our submission to MCSCS, we recommended changes to the regulation so that it would:

- address all street check encounters, including when a police officer is investigating a specific offence
- ensure that police officers notify people of their rights not to answer questions and to disengage
- set limits on how long police may keep street check data and when it must be securely destroyed

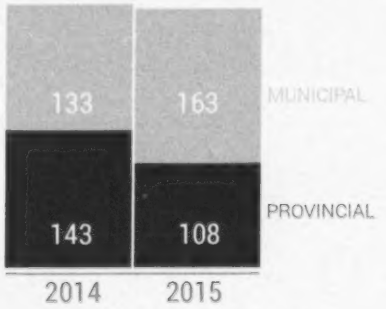
Body-Worn Cameras

Interest in the use of body-worn cameras (BWCs) among Ontario police services is growing. As mobile recording devices,

PRIVACY COMPLAINTS OPENED IN 2015



PRIVACY COMPLAINTS CLOSED IN 2015



BWCs present different challenges from closed circuit television and dashboard camera systems. For example, their mobility increases the amount of personal information captured, including in private places such as people's homes, hospitals and places of worship.

In response to recommendations of former Justice Frank Iacobucci in his report "Police Encounters with People in Crisis," we consulted with and provided advice to the TPS on its BWC pilot project, and are eager to work with any other Ontario police service considering the use of this technology. We look forward to reviewing the results of the TPS pilot project later this year.

Recently, the IPC recommended that the government implement province-wide standards for police use of surveillance technologies, including BWCs, in our submission to the Ministry of Community Safety and Correctional Services, as part of consultations on a Strategy for Safe Communities. In our submission, we also called for clear guidelines around transparency and accountability with respect to the use of surveillance technologies, including data retention and restrictions on secondary use.

"Yes, You Can"

We were pleased to collaborate with a fellow officer of the Legislature, the Provincial Advocate for Children and Youth on a new guide, *Yes, You Can: Dispelling the Myths About Sharing Information with Children's Aid Societies*. This helps professionals working with children understand that privacy legislation does not prevent them from sharing information with a children's aid society (CAS) about a child who may be at risk. In fact, Ontario law requires the disclosure of this important information whenever a professional has reasonable grounds to suspect that a child is in need of protection.

Yes, you can. Ontario law requires the disclosure of information whenever a person has reasonable grounds to suspect that a child is in need of protection.

Health providers, police, teachers, social service workers and other professionals sometimes use privacy as the reason for refusing to disclose information to child protection workers. While often well-intentioned, this refusal may leave a child at risk of harm.

This informative and popular guide clarifies common misunderstandings about privacy, underscores that professionals can disclose information to protect a child from potential harm, and reminds us that privacy should never stand in the way of preventing harm to vulnerable individuals.

Situation Tables

A 'situation table' is a term that refers to regular meetings between representatives from agencies such as police, municipalities, hospitals, social services and schools. The meetings are held to identify and address individual cases that raise concerns about community safety or well-being that one agency cannot address alone.

At these meetings, personal information may be collected, used and disclosed by a wide array of agencies for purposes of harm reduction, often without the individual's consent. While we acknowledge the good intentions, we also know that such an approach can present several risks to privacy rights, including the excessive and unnecessary sharing of personal information.

RECOMMENDATION

Participants in situation tables should use de-identified information and only share personal information on a 'need-to-know' basis. They should be transparent about their information sharing practices.

The IPC is committed to continuing to support situation table participants in addressing community safety and well-being, while protecting privacy. Participants are urged to use de-identified information (information that has been stripped of details that could identify that person) to the greatest extent possible, limit the sharing of personal information to a 'need-to-know' basis, and be transparent about their information sharing practices.

The IPC dialogue with MCSCS and various situation table partners is continuing and our door is open for consultation with any municipality considering the use of similar collaborative practices.

PRIVACY COMPLAINTS

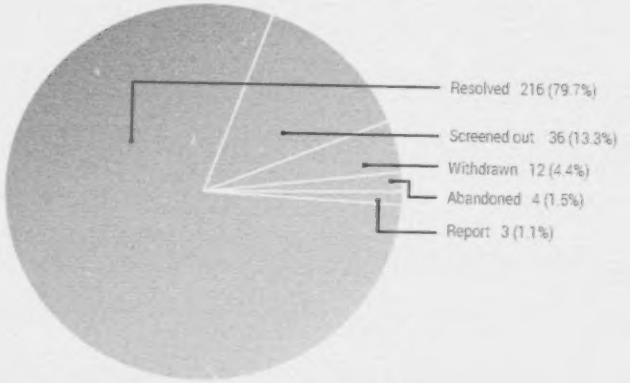
MC13-46
HALTON CATHOLIC DISTRICT SCHOOL BOARD

The use of video surveillance at a school led to a privacy complaint. The IPC found that in using this technology, the school board had not demonstrated that the volume and scope of personal information collected was necessary to the proper administration of a lawfully authorized activity under section 28(2) of *MFIPPA*. The IPC recommended that the school board conduct an assessment of the video surveillance system at the school in a manner consistent with *MFIPPA*, the board's internal policy and the report.

MC13-60
TORONTO CATHOLIC DISTRICT SCHOOL BOARD

Similar to the issues addressed in MC13-46, this privacy complaint also involved the use of video surveillance at a school. The IPC found that the school's collection of personal information within the school property complied with section 28(2) of

PRIVACY COMPLAINTS CLOSED BY TYPE OF RESOLUTION



MFIPPA. However, the collection of personal information by video cameras that were aimed outside the school property did not. The IPC recommended that the school board stop collecting personal information captured by the video surveillance system from outside the school property by modifying what is captured by its cameras, and revise its notice of collection, and its policies, procedures and guidelines.

MC13-67
CITY OF VAUGHAN

The IPC received a complaint alleging that the City of Vaughan contravened *MFIPPA* when making the complainant's contact information available on the Internet in relation to her minor variance application. We found the city to be in compliance with the act, but we recommended that it consider implementing privacy protective measures which would obscure this type of information from search engines and automated agents. We have since issued a guidance paper, *Transparency, Privacy and the Internet: Municipal Balancing Acts*, to further clarify the policy, procedural and technical options municipalities should consider when publishing personal information on the internet.

Key Privacy Publications

To help government organizations understand and meet their obligations under Ontario privacy legislation, the IPC prepared a number of practical guides over the last year.

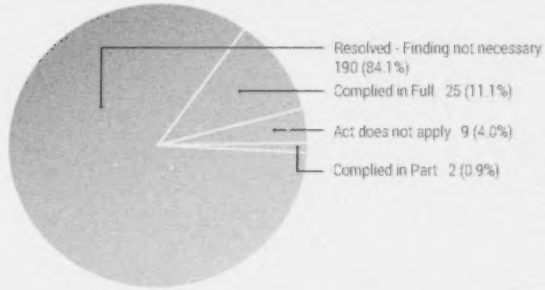
Recognizing the need for advice on conducting surveys in the age of the internet, we released *Best Practices for Protecting Individual Privacy in Conducting Survey Research*. This document details privacy considerations and best practices for the design and implementation of online surveys.

Any public institutions considering new information technologies, systems and programs that may affect privacy are strongly encouraged to complete a privacy impact assessment (PIA). Our *Planning for Success: Privacy Impact Assessment Guide* provides institutions with step-by-step advice on how to carry out a PIA.

Based on the findings of Privacy Complaint *MC13-67*, *Transparency, Privacy and the Internet: Municipal Balancing Acts* describes a number of policy, procedural and technical options available to municipalities to mitigate the privacy risks associated with publishing personal information online.

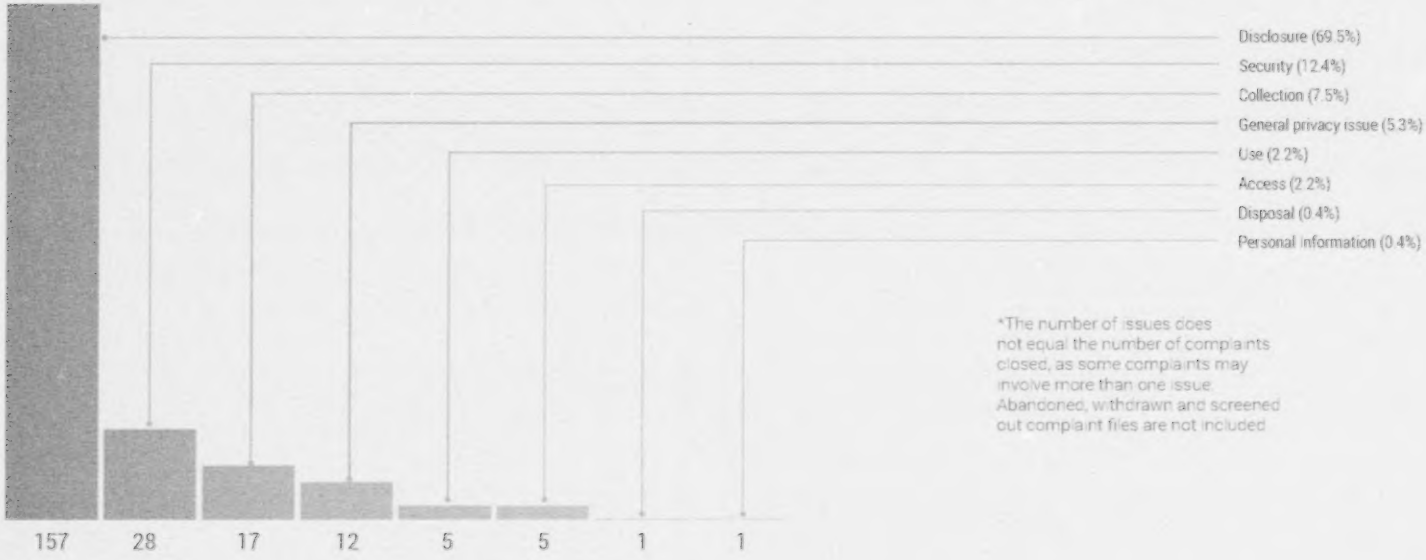
We updated our *Guidelines for the Use of Video Surveillance* to support compliance with the requirements of *FIPPA* and *MFIPPA* regarding the collection, use, retention and disclosure of personal information. The guidelines discuss how these requirements apply to video surveillance technologies.

OUTCOME OF ISSUES* IN PRIVACY COMPLAINTS



*The number of issues does not equal the number of complaints closed, as some complaints may involve more than one issue. Abandoned, withdrawn and screened out complaint files are not included.

ISSUES* IN PRIVACY COMPLAINTS



*The number of issues does not equal the number of complaints closed, as some complaints may involve more than one issue. Abandoned, withdrawn and screened out complaint files are not included.

PHIPA: A Prescription for Privacy

A patient's personal health information (PHI) is perhaps the most sensitive information about them; Ontarians trust that doctors, nurses and other health professionals make every effort to protect it. Patient privacy is integral to the delivery of health care and must be embedded into the culture of health care organizations. While hospitals and other health care providers have taken steps to ensure that patient privacy is protected, unauthorized access to PHI, for purposes including curiosity or personal gain, appears to be a continuing problem in Ontario's health sector.

This year, our office was actively engaged in raising awareness about patient privacy and protecting health information, and addressed a number of complaints about breaches where PHI was accessed for unauthorized purposes.

The Personal Health Information Protection Act (PHIPA) *governs the manner in which your personal health information (PHI) may be collected, used and disclosed within the health sector. It regulates health information custodians (custodians), as well as individuals and organizations that receive PHI from custodians.*

On January 28 our office held a special privacy day event, *PHIPA*: A Prescription for Privacy, where we led discussions on unauthorized access (commonly called "snooping") and how to reduce this risk to patient privacy. To help prevent incidents of unauthorized access, our office used this occasion to launch our "Is it Worth it?" campaign, which included the release of our paper, Detecting and Deterring Unauthorized Access to Personal Health Information.

This campaign shed light on the extent of the problem and provided guidance to custodians on lowering the risk of unauthorized access. One way of reducing this risk is by developing and implementing detailed policies that are clear about the obligations of health care providers to protect health records, and procedures they should follow to ensure they do.

The stakes are high. The impacts of unauthorized access are real and can have lasting consequences for health care providers, patients and the entire health sector, including the potential emotional harm to people whose privacy is violated. Damage to professional reputations and disciplinary action by regulatory colleges are additional consequences of unauthorized access.

Is it worth it? Unauthorized access can result in emotional harm to people whose privacy is violated, damage to professional reputations, and disciplinary action from regulatory colleges.

Respect for patient privacy is critical to building and maintaining trust in the health sector. Custodians and their agents must, and in most cases do, take patient privacy seriously. Together, we must continue to send a strong message that unauthorized access is unacceptable and will not be tolerated.

Protecting Patient Privacy

In June, our office was pleased to participate in an information session held by The Ottawa Hospital, as part of the hospital's privacy awareness week. Similar to our *PHIPA*: A Prescription for Privacy event, the theme of this session was 'Protecting Patient Privacy from Unauthorized Access by Custodians or their Agents.'

In the spirit of this partnership with The Ottawa Hospital, our office is committed to working with frontline providers on raising awareness about this very important issue. We look forward to further collaboration on strategies to ensure that patient privacy is respected and preserved.

SUMMARY OF *PHIPA* COMPLAINTS

-13% ACCESS/CORRECTION OPENED 2015 97 2014 111	-2.5% INDIVIDUAL OPENED 2015 117 2014 120	+3% SELF-REPORTED BREACH OPENED 2015 178 2014 172	+89% IPC INITIATED OPENED 2015 68 2014 36
-20% ACCESS/CORRECTION CLOSED 2015 84 2014 105	+13% INDIVIDUAL CLOSED 2015 105 2014 93	+3% SELF-REPORTED BREACH CLOSED 2015 175 2014 170	+119% IPC INITIATED CLOSED 2015 68 2014 31

e-PHIPA (Bill 119)

In 2015, we were pleased that the Ontario Minister of Health and Long-Term Care, Eric Hoskins, moved forward with all the IPC's recommendations for amendments to *PHIPA*, and introduced Bill 119, the *Health Information Protection Act, 2015*, to improve accountability in Ontario's health care system and improve patient privacy.

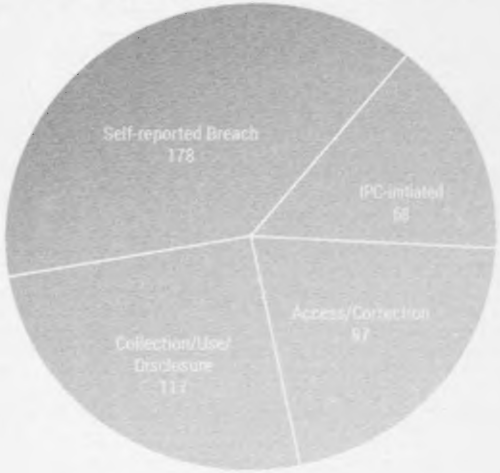
Bill 119 would enhance the protection of patients' health information by establishing a provincial governance framework for shared electronic records. It would also:

- mandate the reporting of health privacy breaches to our office and relevant regulatory colleges
- remove the six-month limitation period for starting prosecutions
- double the maximum fines to $100,000 for a person ($250,000 for organizations) found to have committed offences under *PHIPA*

Once Bill 119 is in effect, we will work with the Ministry of Health and Long-Term Care on the implementation of these important amendments that will strengthen privacy and accountability for all Ontarians.

Bill 119 also rewrote the *Quality of Care Information Protection Act* (*QCIPA*). The IPC proposed a simple amendment that would ensure that it could carry out its oversight

SUMMARY OF *PHIPA* COMPLAINTS OPENED



function and have explicit authority to conduct an independent review of decisions to refuse to provide access to records that are believed to contain "quality of care information." These reviews would help to assure individuals that they have been provided with access to all of the information to which they are entitled. It would also help to alleviate public concerns about the lack of transparency and oversight for incidents reviewed under the proposed legislation.

We were disappointed this common sense amendment was rejected.

Simplified *PHIPA* Processes

Seeing that *PHIPA* matters are resolved in a fair, just and timely manner was a key part of our work in 2015. We looked at our different processes and made changes to ensure that they are clear and simple to follow, and streamlined our approach to managing the different types of complaints under the act.

As part of these improvements, we will:

- follow a similar process for all types of public complaints, whether they are access or privacy related
- distinguish, in our process, between complaints that are initiated by the public, and those initiated by the IPC and those reported by a health care provider
- clarify roles and responsibilities of the Intake, Investigation/Mediation, and Adjudication areas, so the three stages of our tribunal process are clear

Significant *PHIPA* Decisions

This year, our office also began publishing an expanded range of *PHIPA* decisions, which include those that:

- follow a review and contain orders or recommendations
- follow a review and make no orders or recommendations
- are interim decisions
- are decisions not to conduct a review

Publishing these decisions will provide greater guidance to the health care community and the public about their rights and obligations.

In *PHIPA* Decision 15, we found that for the purposes of preparing a custody and access assessment report, a psychologist was not a "health information

A "health information custodian" as defined in section 3(1) of* PHIPA, *is premised on the fact that a custodian must be providing health care.

custodian" as defined in section 3(1) of *PHIPA*, which is premised on the fact that the person must be providing health care. Further, the term "health care" as defined in section 2 of *PHIPA* must be for a "health-related purpose."

Because we found that the psychologist was not providing health care, the complainant did not have a right to request a correction under *PHIPA*.

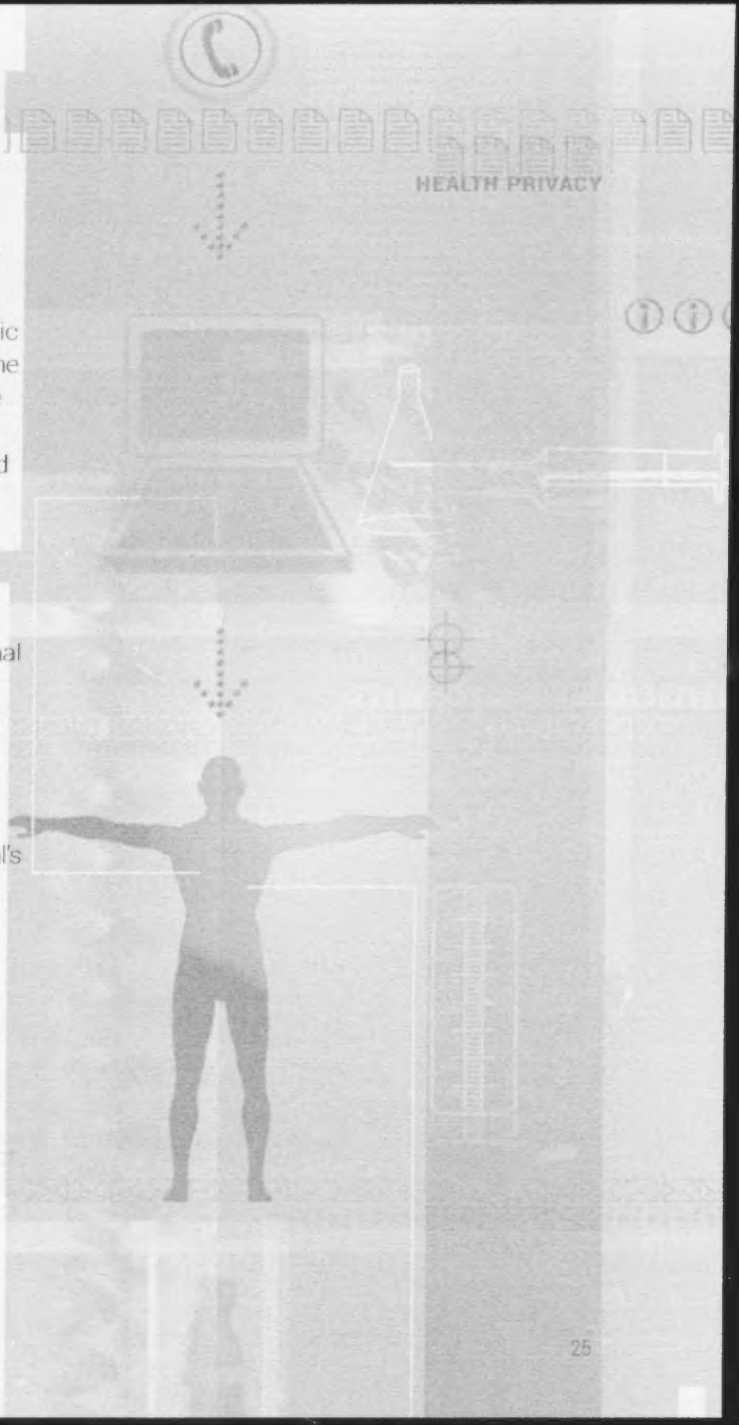
In *PHIPA* Decision 16, the IPC refused a request by a doctor to defer the IPC's review of a privacy complaint under *PHIPA*, pending the completion of related proceedings before the College of Physicians and Surgeons of Ontario. The review was allowed to proceed because it would not be in the interest of fairness to defer it for an indefinite period.

In *PHIPA* Decision 17, the IPC found that the complainant's request for records of his wife and daughter's personal health information is governed by *PHIPA*, and his request for his own personal information is governed by *FIPPA*. The IPC upheld the hospital's decision to refuse access to most of the information at issue on the basis of exclusions and exemptions in *PHIPA* and *FIPPA*. Specifically, we found that the public interest override in *FIPPA*—which allows the disclosure of records that could otherwise be withheld under certain exemptions in *FIPPA*—does not apply, and we also upheld the hospital's exercise of discretion under both acts.

In *PHIPA* Decision 18, the complainant requested that the IPC review a hospital's search for records, in the belief that additional records should exist. Our office asked for and received an affidavit from the hospital's manager of health records and privacy, outlining the steps that were taken to locate the responsive records. Based on the evidence, the adjudicator upheld the hospital's search and dismissed the complaint.

New Health Privacy Publications

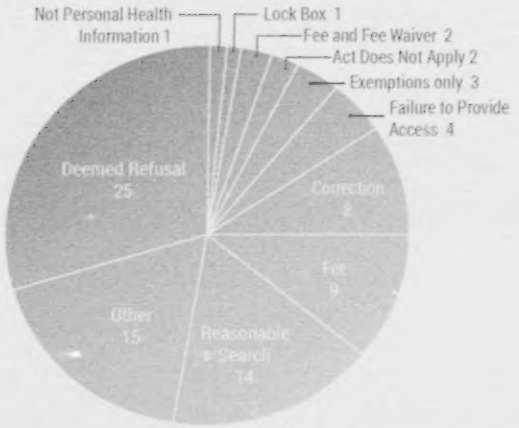
In 2015, our office updated our existing *Frequently Asked Questions (FAQ): Personal Health Information Protection Act*



paper and our fact sheet on health cards and health numbers.

The FAQ and fact sheet have a new look and feel, and easy-to-understand, gender-neutral language. The updated FAQ includes more in-depth guidance on such issues as disclosing personal health information in an emergency, getting the health records of deceased relatives, and notification requirements in the event of a privacy breach. The revised fact sheet on health cards and health numbers clarifies who may collect, use or disclose health numbers, and under what circumstances, and whether health cards can serve as a voluntary proof of identity.

ACCESS/CORRECTION COMPLAINTS CLOSED BY ISSUE



TYPES OF *PHIPA* COMPLAINT FILES OPENED IN 2015

1. Public Hospital: 127
2. Clinic: 78
3. Other: 57
4. Doctor: 47
5. Community or Mental health centre, program or service : 27
6. Community Care Access Centre: 20
7. Other health care professional: 19
8. Pharmacy: 18
9. Independent Health Facility: 15
10. Ministry of Health: 8
11. Other prescribed person: 6
12. Laboratory: 5
13. Dentist: 4
14. Health Data Institute: 4
15. Ambulance services: 3
16. Institution - Mental Hospitals Act: 3
17. Agent: 2
18. Home or joint home (aged or rest): 2
19. Long-term care facility: 2
20. Psychiatric Facility: 2
21. Board of Health: 1
22. Charitable home for the aged: 1
23. Chiropractor: 1
24. Home for special care: 1
25. Minister of Health: 1
26. Nurse: 1
27. Pharmacist: 1
28. Private Hospital: 1
29. Psychologist: 1
30. Recipient: 1
31. Social Worker: 1

Mediation: Success Behind the Scenes

While our office's orders and decisions receive most of the public's attention, a large number of access to information appeals and privacy complaints are resolved through mediation. Below are some examples of resolutions achieved through mediation:

- An individual filed a complaint against a hospital alleging that a doctor's employee had accessed and then disclosed his health records during a court proceeding, without his consent. The hospital and the doctor participated in the mediation process and agreed to take a number of steps to address the privacy breach, including: disciplining the employee; improving policies, procedures and training; and putting in place additional measures and auditing functions to protect patients' information. On receiving an apology letter and details of the steps that were taken in response to the breach, the individual was satisfied with the results of mediation.

- A police service denied a reporter's request for a copy of its tenure review. During mediation, the police agreed to review the record to determine whether any information could be disclosed. The police invited the journalist to contact the acting superintendent responsible for the tenure review, which led to a meeting to discuss the details of her request. As a result of this meeting, the reporter got the information she was looking for.

- A reporter asked a city for invoices and supporting documents detailing the amount paid to a law firm over a seven-year period. The request was denied on the basis of solicitor-client privilege. During mediation, the journalist and the city participated in a teleconference where the reporter said that he would be satisfied with receiving the totals from each invoice, as well as the annual totals paid. The city agreed to create a record containing that information and issued a revised decision, which settled the appeal.

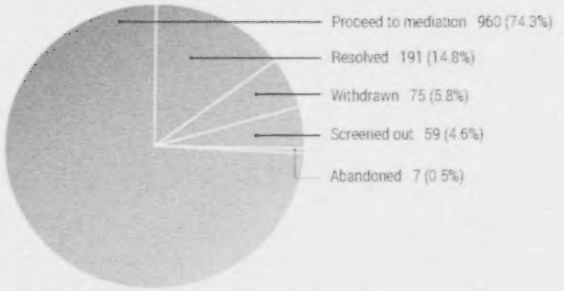
- A city received a request for records relating to licensing of four properties. The city granted partial access, but withheld certain records on the basis of solicitor-client privilege, among other things. During mediation, the city provided the requester with a detailed index of records so that he could better assess the application of solicitor-client privilege. On reviewing the index, the requester was satisfied with the information provided.

- Three people took issue with a police service's practice of including non-criminal/mental health information in police record checks on individuals who are applying to work with vulnerable

Our mediators and analysts are always working to find a resolution that satisfies the needs of all involved. In fact, most appeals in 2015 were fully settled without the need to proceed to adjudication, saving significant time and resources for all parties.

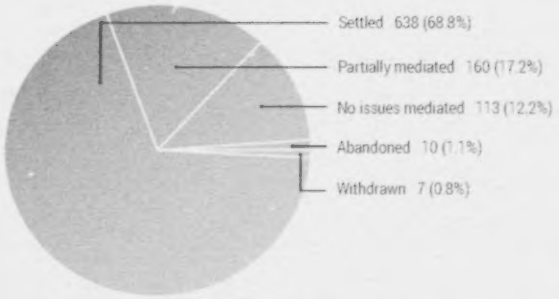
OUTCOME OF APPEALS BY STAGE CLOSED

APPEALS PROCESSED* IN INTAKE BY DISPOSITION



* "Processed" refers to those appeals that completed the Intake stage somewhere between January 1, 2015 and December 31, 2015 and includes files that are still open in the Mediation and Adjudication stages.

APPEALS PROCESSED* IN MEDIATION BY DISPOSITION



* "Processed" refers to those appeals that completed the Mediation stage somewhere between January 1, 2015 and December 31, 2015 and includes files that are still open in the Adjudication stage.

people. They were concerned that the mental health information the police had collected may have been uploaded into the CPIC database and shared with U.S. border personnel. During mediation, the police issued a new record check to each of the three individuals, excluding this type of information, and advised that they would be changing their policy. The police confirmed in a letter that this information would not be available to U.S. Customs and Border Protection, and the complainants were satisfied with this response.

- A town received a request from the media for a copy of a licencing agreement related to a music festival. Based on an objection from a party to the agreement, the town denied access. After discussions with the mediator about IPC decisions in similar cases, the party consented to disclosure of the agreement.
- A request was made to a provincial institution for documents associated with the wind up of a specified pension plan. The institution issued a decision denying access on the basis that no records existed. The mediator arranged a teleconference with the requester, the FOI coordinator, a program area representative and a legal advisor. During this meeting, the institution provided the requester with an explanation as to why certain records did not exist and provided him with information to redirect his request, which satisfied the requester.

Consultations: Legislation, Programs and Information Practices

In keeping with our focus on outreach, engagement and collaboration, the IPC actively participated in a number consultations during 2015, in addition to advising on legislative amendments and regulations. Some organizations we worked with include:

TORONTO TRANSIT COMMISSION
- Forward-facing cameras on transit vehicles

LIQUOR CONTROL BOARD OF ONTARIO
- Application for indirect collection of personal information for online sales

MINISTRY OF COMMUNITY SAFETY AND CORRECTIONAL SERVICES
- Bill 113—*Police Record Checks Reform Act, 2015*
- Guidance on Information Sharing in Multi-Sectoral Risk Intervention Models (Situation Tables)
- *Police Services Act* Street Check Regulation

PROVINCIAL ADVOCATE FOR CHILDREN AND YOUTH
- Joint Guidance—Yes, You Can: Information Sharing with Children's Aid Societies

MINISTRY OF FINANCE
- Bill 173—*Jobs for Today and Tomorrow Act (Budget Measures), 2016*—schedule to the *Benefits Administration Integration Act, 2016*
- Bill 91—*Building Ontario Up Act (Budget Measures), 2015*—Amendments to the *Assessment Act*

INDEPENDENT ELECTRICITY SYSTEM OPERATOR
- Foundation Working Group—Rules and Protocols for Access to Smart Meter data

LEGAL AID ONTARIO
- Open Government consultation paper

TREASURY BOARD SECRETARIAT
- Local Poverty Reduction Fund
- Open Government
- Open Data Directive
- Open Data Guidebook
- Open Information

MINISTRY OF ENERGY
- Meter Data Management and Repository Data Access Platform Advisory Committee
- Green Button Natural Gas Working Group
- Proposed Energy and Water Reporting and Benchmarking Initiative for Large Buildings

MINISTRY OF GOVERNMENT AND CONSUMER SERVICES
- Taking the Right Steps—A Guide to Managing Privacy and Privacy Breaches
- Recordkeeping Amendments to *FIPPA* and *MFIPPA* Information Sheet
- Guide to Electronic, Paper and other Records Searches

ONTARIO PROVINCIAL POLICE
- Automatic Licence Plate Recognition Program

TORONTO POLICE SERVICE
- Pilot project on the use of Body Worn Cameras

Commissioner's Recommendation: Modernize Ontario's Privacy and Access Legislation

It has been almost thirty years since *FIPPA* and *MFIPPA* came into force. Since that time, public expectations, technologies and the ways in which government does business have changed. In other provinces, access and privacy laws have been strengthened to meet the challenges of modern society. It is time for Ontario to do the same. We are calling on the Ontario government to undertake a comprehensive review of *FIPPA* and *MFIPPA* through an open process that encourages public participation. Now is the time to update the acts and ensure that the access and privacy rights of Ontarians are protected in our changing environment.

Expand Coverage Under the Act

Since the acts were introduced, government has changed the way it delivers public services. Increasingly, services are outsourced or delivered by public-private partnerships, arms-length agencies, delegated administrative authorities, self-funded agencies, or other service delivery models. Regardless of their status, these organizations are responsible for delivering services to the public and have corresponding duties and responsibilities.

Decisions about which organizations are covered by the acts have been made on a case-by-case basis and at various points in time, resulting in inconsistent levels of accountability and transparency.

Unless there are unique and compelling reasons not to, an organization should be covered under the acts if:

- it receives a significant amount of its operating funds from the government
- it delivers a program designed to support government objectives
- the government plays a significant role in its policy development and operational direction

FIPPA and *MFIPPA* should be amended to ensure a consistent approach that allows for the creation of new service delivery models that do not weaken access and privacy rights.

Amend the Acts to Address Changing Communication and Information Technologies

New technologies have also changed the way we share, analyze and store information. It is critical that a review of the acts examine and deal with the impact of technology on access and privacy rights.

For example, the widespread use of instant messaging, and personal devices and accounts, creates a risk that business records are not properly created and stored. This could mean that information

that should be available to people who request it is lost.

In January 2015, Canada's information and privacy commissioners issued a joint statement calling on their respective governments to create a legislated "duty to document." A review of *FIPPA* and *MFIPPA* would allow Ontario to respond to this call for action by including a duty to document business-related activities accompanied by effective oversight and enforcement.

New technology has also allowed for the growth of large-scale databases, and the ability to combine and analyze data as never before. This computing power—coupled with increased capacity for data sharing within and between institutions, levels of governments, across jurisdictions, and within public-private partnerships—means that there are new privacy risks that need to be addressed.

In other jurisdictions, access and privacy laws have been amended to allow for collection and disclosure of personal information to support service delivery programs that involve multiple agencies, and data sharing to support research and evidence-based decision making.

A comprehensive review of the acts would help address:

- the need for collaborative service delivery models and data sharing to support research and analysis
- public expectations about access to information and services online
- the need to ensure that new technologies are used in a transparent and accountable manner, and that they do not negatively impact access and privacy rights

Expand the Commissioner's Order-Making Power

While *FIPPA* and *MFIPPA* give the IPC order-making power in relation to access requests, under the current legislation, this power is not extended to privacy complaints.

Our powers are limited to ordering an institution to stop a collection practice and to destroy collections of personal information that contravene the acts. In investigating issues other than collection practices, such as allegations of improper use, disclosure, retention and destruction of information, we can only issue recommendations and not a binding order.

Having the power to investigate and make orders in relation to privacy is a power that exists in many other modern privacy statutes, including *PHIPA*, Ontario's health privacy legislation. We know that order-making power deters institutions from behaviour that is not in compliance with *FIPPA* and *MFIPPA*, and provides a strong incentive and motivation for settlement. The Commissioner is therefore calling for amendments to *FIPPA* and *MFIPPA* to expand the IPC's order-making power to include all potential privacy complaints.

Recently, we were forced to start a court proceeding to enforce recommendations we made in a privacy complaint report. Amending the acts to authorize our office to issue an order at the end of a privacy

investigation would enable our office to more effectively protect the privacy rights of all Ontarians.

Mandatory Proactive Disclosure of Identified Categories of Records

In previous annual reports, we called for greater openness, transparency and accountability through the routine and proactive disclosure of government records. Proactive disclosure supports the public's right to access information, and is a key part of Open Government.

Legislation in other provinces addresses the need for proactive disclosure. For example, British Columbia's public sector access and privacy legislation requires public bodies to establish categories of records, such as travel and hospitality expenses and calendars of senior officials, that are available to the public without a request. Similarly, Quebec's public sector access and privacy laws include a list of specific information that public bodies must proactively disclose.

To further modernize *MFIPPA* and *FIPPA*, the acts should be amended to require that categories of records be identified for proactive disclosure, including, for example, procurement records. Each year, we receive a number of appeals regarding requests for access to contracts awarded by institutions. The public has a right to be informed about the procurement process, including how contracts are awarded, what has been contracted for, how the successful bidders were chosen, what the various costs of the contract are, and who is responsible for the decision-making relating to the contract.

Ontario was one of the first provinces in Canada to create access and privacy legislation. Since then, societal expectations, technology and government have evolved, but the acts have remained relatively unchanged. Now, *FIPPA* and *MFIPPA* lag behind the standards established in other Canadian jurisdictions. It is time to ensure that the access and privacy rights of Ontarians align with the rights of other Canadians.

YEAR AT A GLANCE

PROVINCIAL

PERSONAL INFORMATION	GENERAL RECORDS	TOTAL
-11% REQUESTS **2015 7,367** 2014 8,241	-6% REQUESTS 2015 15,584 2014 16,666	-5% TOTAL REQUESTS **2015 22,951** 2014 24,907
-8% APPEALS OPENED **2015 179** 2014 194	+7% APPEALS OPENED 2015 536 2014 501	+3% TOTAL APPEALS OPENED **2015 715** 2014 695
-7% APPEALS CLOSED **2015 186** 2014 201	+2% APPEALS CLOSED 2015 506 2014 497	-1% TOTAL APPEALS CLOSED **2015 692** 2014 698
+199% AVERAGE COST **2015 $13.37** 2014 $4.47	-7% AVERAGE COST 2015 $38.67 2014 $41.49	

MUNICIPAL

PERSONAL INFORMATION	GENERAL RECORDS	TOTAL
+0.1% REQUESTS **2015 18,492** 2014 18,481	+10% REQUESTS 2015 18,367 2014 16,648	+5% TOTAL REQUESTS **2015 36,859** 2014 35,129
-4% APPEALS OPENED **2015 210** 2014 219	+18% APPEALS OPENED 2015 478 2014 406	+10% TOTAL APPEALS OPENED **2015 688** 2014 625
-18% APPEALS CLOSED **2015 209** 2014 255	+1% APPEALS CLOSED 2015 428 2014 423	-6% TOTAL APPEALS CLOSED **2015 637** 2014 678
+7% AVERAGE COST **2015 $9.49** 2014 $8.86	-1% AVERAGE COST 2015 $25.69 2014 $25.93	

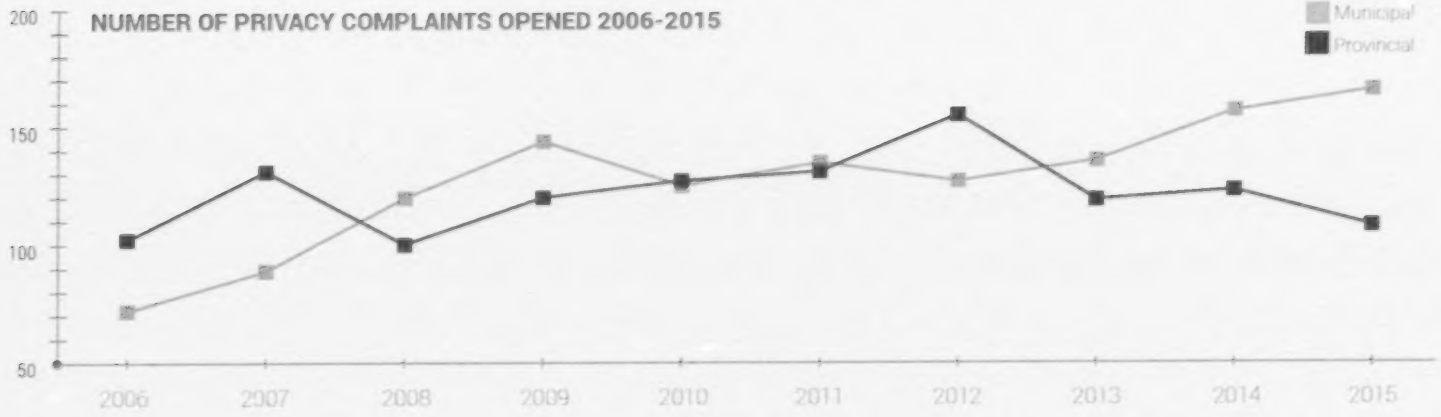
YEAR AT A GLANCE

PRIVACY COMPLAINTS

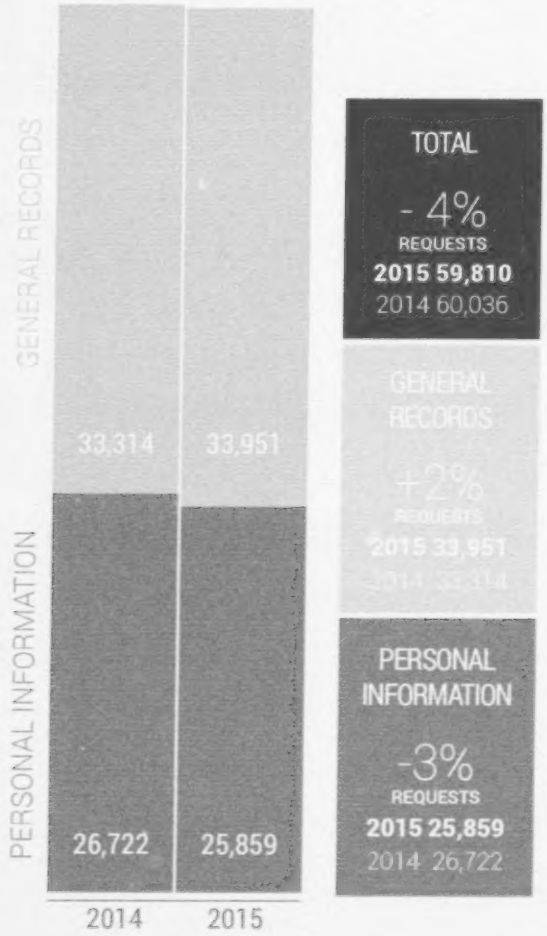
PROVINCIAL	MUNICIPAL
-11%	+6%
OPENED	OPENED
2015 109	**2015 167**
2014 123	2014 157
-24%	+23%
CLOSED	CLOSED
2015 108	**2015 163**
2014 143	2014 133

SUMMARY OF PHIPA COMPLAINTS

-13%	-2.5%	+3%	+89%
ACCESS/CORRECTION OPENED	INDIVIDUAL OPENED	SELF-REPORTED BREACH OPENED	IPC INITIATED OPENED
2015 97	**2015 117**	**2015 178**	**2015 68**
2014 111	2014 120	2014 172	2014 36
-20%	+13%	+3%	+119%
ACCESS/CORRECTION CLOSED	INDIVIDUAL CLOSED	SELF-REPORTED BREACH CLOSED	IPC INITIATED CLOSED
2015 84	**2015 105**	**2015 175**	**2015 68**
2014 105	2014 93	2014 170	2014 31



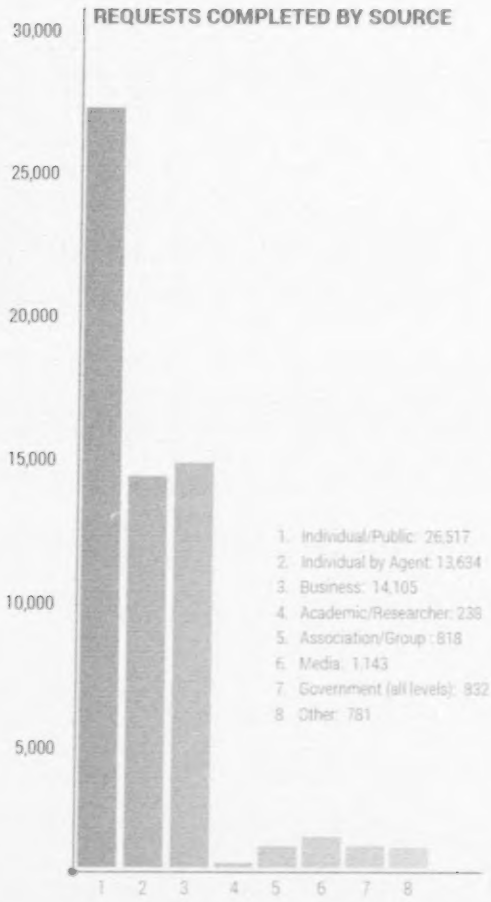
OVERALL REQUESTS

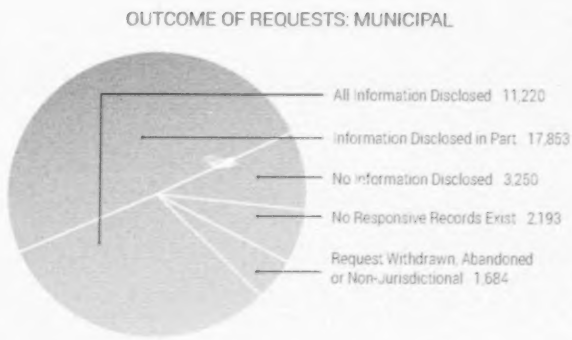


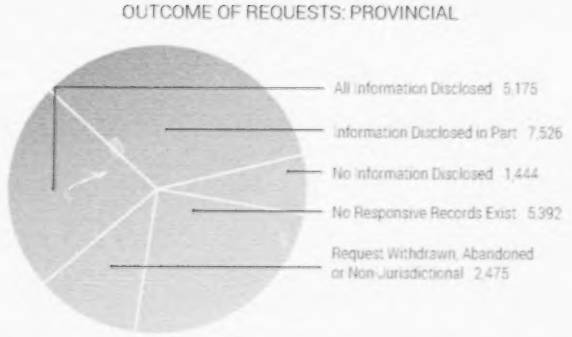
TOTAL
- 4%
REQUESTS
2015 59,810
2014 60,036

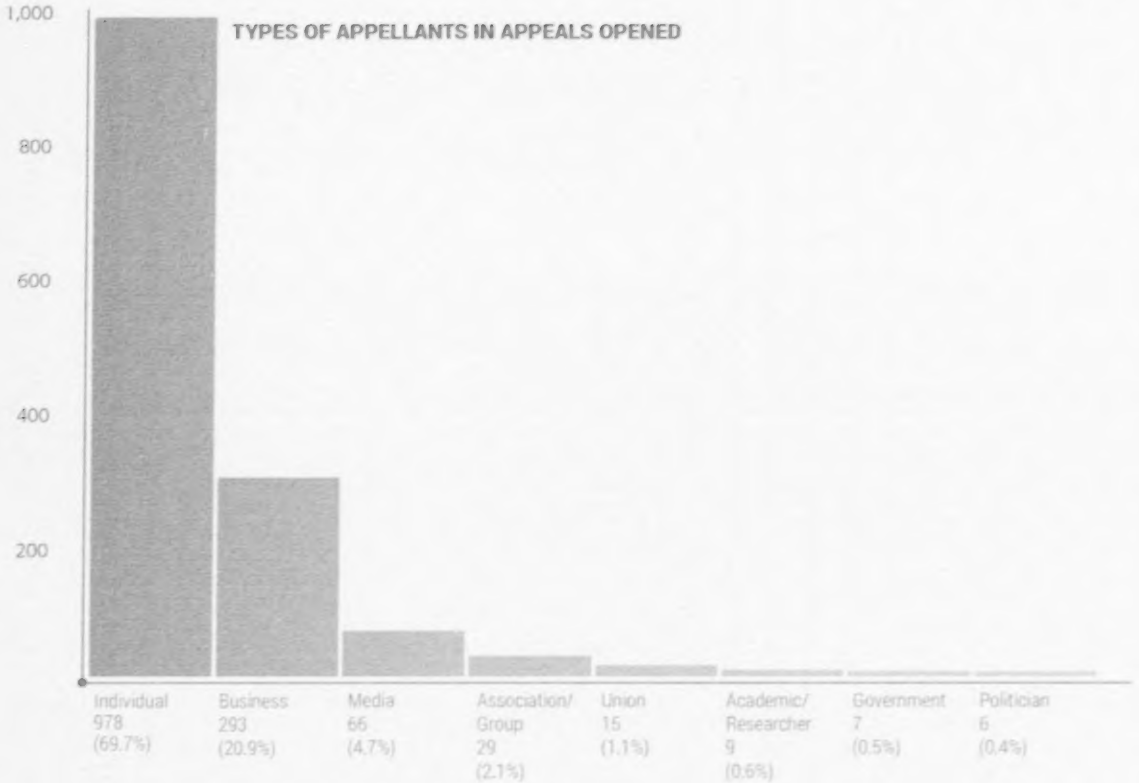
GENERAL RECORDS
+2%
REQUESTS
2015 33,951
2014 33,314

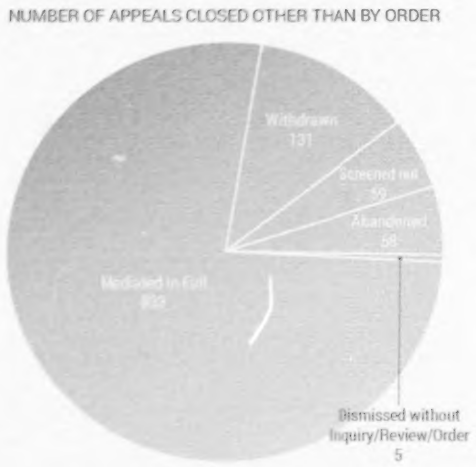
PERSONAL INFORMATION
-3%
REQUESTS
2015 25,859
2014 26,722

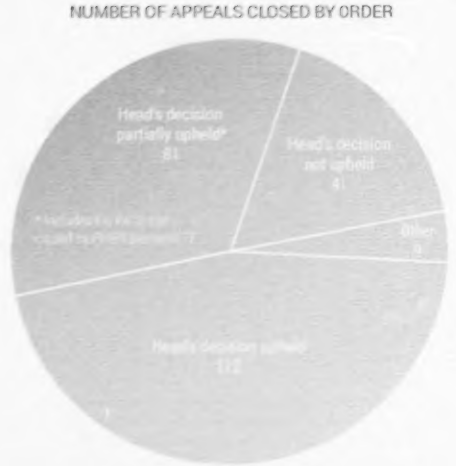



OUTCOME OF REQUESTS: MUNICIPAL
All Information Disclosed 11,220
Information Disclosed in Part 17,853
No Information Disclosed 3,250
No Responsive Records Exist 2,193
Request Withdrawn, Abandoned or Non-Jurisdictional 1,684

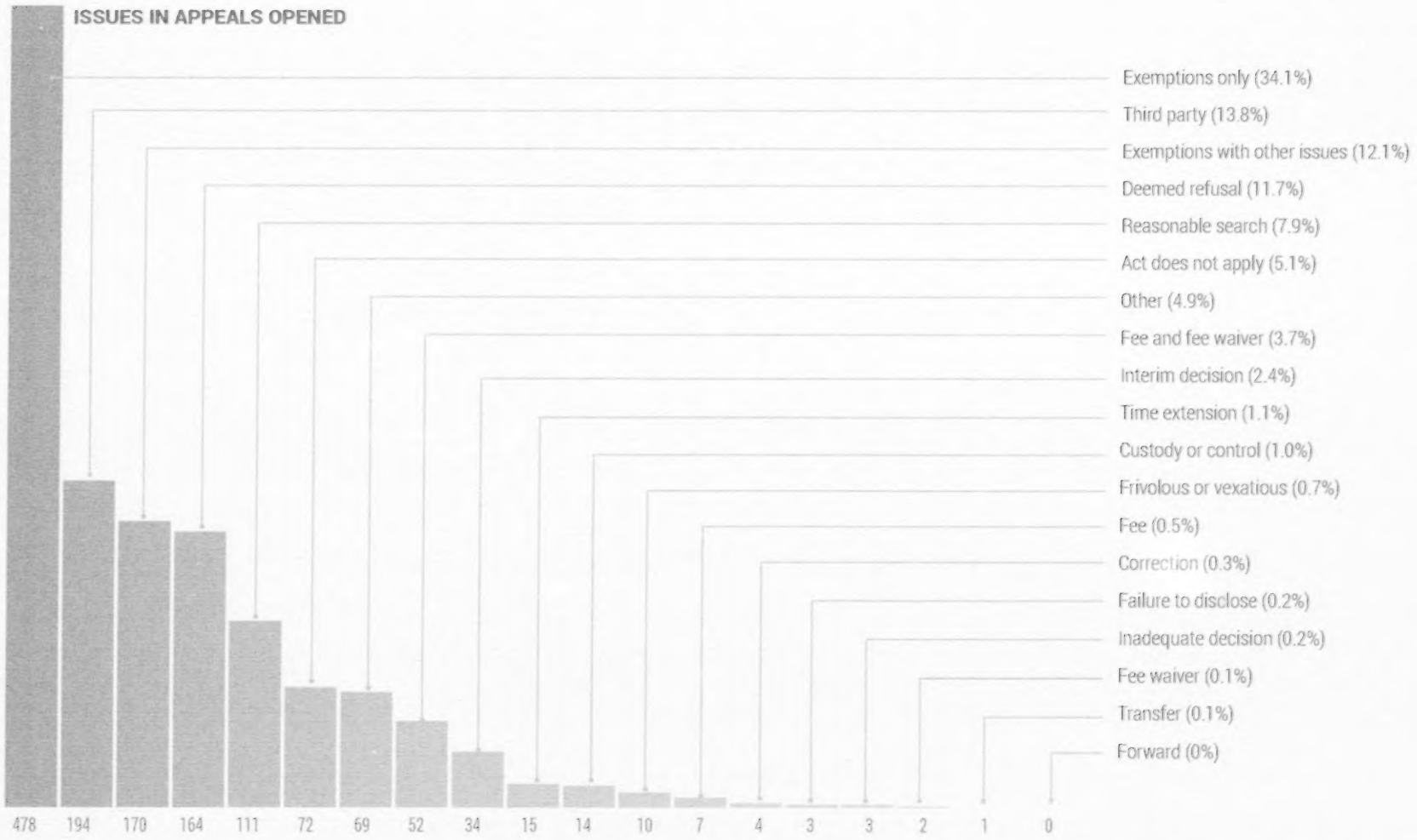

OUTCOME OF REQUESTS: PROVINCIAL
All Information Disclosed 5,175
Information Disclosed in Part 7,526
No Information Disclosed 1,444
No Responsive Records Exist 5,392
Request Withdrawn, Abandoned or Non-Jurisdictional 2,475


TYPES OF APPELLANTS IN APPEALS OPENED
1,000
800
600
400
200
Individual 978 (69.7%)
Business 293 (20.9%)
Media 65 (4.7%)
Association/ Group 29 (2.1%)
Union 15 (1.1%)
Academic/ Researcher 9 (0.6%)
Government 7 (0.5%)
Politician 6 (0.4%)


NUMBER OF APPEALS CLOSED OTHER THAN BY ORDER
Withdrawn 131
Abandoned 58
Mediated in Full 93
Dismissed without Inquiry/Review/Order 5

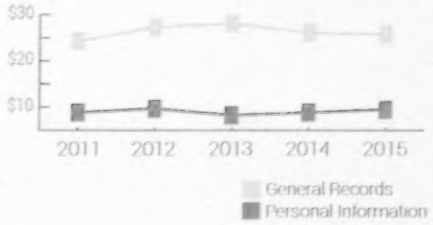

NUMBER OF APPEALS CLOSED BY ORDER
Head's decision partially upheld* 81
Head's decision not upheld 41
Other 9

ISSUES IN APPEALS OPENED



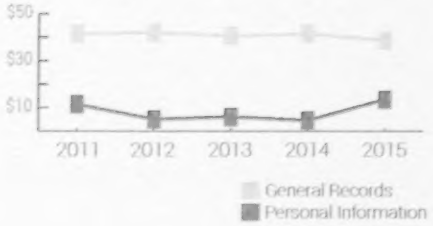
AVG COST OF MUNICIPAL REQUESTS

PERSONAL INFORMATION	GENERAL RECORDS
$9.49	$25.69
2015	2015



AVG COST OF PROVINCIAL REQUESTS

PERSONAL INFORMATION	GENERAL RECORDS
$13.37	$38.67
2015	2015



TOTAL FEES COLLECTED AND WAIVED

MUNICIPAL	PROVINCIAL	TOTAL
$184,471.30 TOTAL APPLICATION FEES COLLECTED 2015	$120,561.76 TOTAL APPLICATION FEES COLLECTED 2015	$305,033.06 TOTAL APPLICATION FEES COLLECTED 2015
$450,105.67 TOTAL ADDITIONAL FEES COLLECTED 2015	$545,697.96 TOTAL ADDITIONAL FEES COLLECTED 2015	$995,803.63 TOTAL ADDITIONAL FEES COLLECTED 2015
$634,576.97 TOTAL 2015	$666,259.72 TOTAL 2015	$1,300,836.69 TOTAL 2015
$44,533.93 TOTAL FEES WAIVED 2015	$24,146.20 TOTAL FEES WAIVED 2015	$68,680.13 TOTAL FEES WAIVED 2015

Financial Statement

	2015-2016 Budget $	2014-2015 Budget $	2014-2015 Actual $
SALARIES AND WAGES	10,444,100	10,444,100	8,880,278
EMPLOYEE BENEFITS	2,401,900	2,625,900	1,982,594
TRANSPORTATION AND COMMUNICATIONS	337,500	337,500	187,305
SERVICES	1,960,300	1,960,300	2,145,339
SUPPLIES AND EQUIPMENT	336,000	336,000	336,690
TOTAL	**15,479,800**	**15,703,800**	**13,532,206**

Note: The IPC's fiscal year begins April 1 and ends March 31.

The financial statement of the IPC is audited on an annual basis by the Office of the Auditor General of Ontario.

2015 Appeals Fees Deposit

(Calendar year)

GENERAL INFO.	PERSONAL INFO.	TOTAL
$18,550	$2,760	$21,310

HOW TO REACH US

Information and Privacy Commissioner of Ontario
2, Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8

Toronto area: 416-326-3333
Long distance: 1-800-387-0073 within Ontario
TDD/TTY: 416-325-7539

www.ipc.on.ca
info@ipc.on.ca